Incident Response Report Template

Incident Response Report Template

Incident Response Report

Incident ID:
[Unique identifier for the incident]

Incident Date and Time:
[When the incident was first detected or reported]

Incident Description:
[A brief overview of the incident (e.g., unauthorized access, DDoS attack, data breach, etc.)]

Incident Severity Level:
[Choose severity: Low / Medium / High / Critical]

Incident Category:
[Select the appropriate category: e.g., Network Attack, Web Application Attack, System Compromise, Malware, etc.]

Affected Systems:
[List the systems, applications, or services affected by the incident]

Impact Assessment:
[Describe the impact on business operations, services, customers, etc.]

Incident Timeline

Time	Action Taken	Person Responsible
[HH]	[First action taken, e.g., detected vulnerability]	[Name/Role]
[HH]	[Containment action, e.g., isolating affected system]	[Name/Role]
[HH]	[Eradication steps, e.g., patching vulnerabilities]	[Name/Role]
[HH]	[Recovery action, e.g., restoring from backups]	[Name/Role]

Time	Action Taken	Person Responsible
[HH]	[Final action, e.g., monitoring, validation]	[Name/Role]

Detection Methods:

[Explain how the incident was detected (e.g., monitoring tools, user report, IDS alert, etc.)]

Containment Measures Taken:

[Describe the steps taken to contain the incident, such as isolating affected systems, blocking malicious IPs, disabling compromised accounts, etc.]

Eradication Measures Taken:

[Explain what was done to remove the threat or fix vulnerabilities, e.g., patching, restoring from clean backups, deleting malware, etc.]

Recovery Process:

[Detail the steps taken to restore normal service operations, such as restoring data, services, systems, and the timeline for recovery.]

Communication:

- **Internal Communication**: [Who was notified within the organization, including timelines]
- **External Communication**: [Who was informed externally (e.g., customers, regulatory bodies, vendors), if applicable]

Root Cause Analysis:

[If available, provide a brief analysis of the root cause of the incident, such as a vulnerability, misconfiguration, or human error.]

Incident Resolution:

[State whether the incident has been fully resolved or is still ongoing.]

Next Steps and Follow-up Actions:

[Outline any actions that need to be taken after the incident, such as further investigation, system hardening, etc.]